

**I. PURPOSE:**

This Administrative Directive establishes a general framework for securing the electronic assets of the City, and provides guidance for specific security issues that have general application in the City's technology environment. This directive supports and supplements Administrative Directive 7.5 – Acceptable Use of Information Technology. Nothing in this directive supersedes provisions of Directive 7.5.

**II. POLICY:**

- A. The City's computing and technology environment, along with the data it creates and maintains is a valuable asset. The City will take all reasonable and necessary measures to maintain the availability, dependability and integrity of that environment. The City will analyze risks carefully to maintain a proper balance between security measures and the requirement that its technology environment effectively and efficiently support its operations.
- B. The Information Technology Services Department has primary responsibility for security of the City's electronic systems, and may establish such policies, procedures and standards as may be necessary to assure the security of City systems. ITSD shall develop and maintain a comprehensive security program for the City, and shall provide guidance and advice to technology users in maintaining appropriate security.
- C. All technology users are responsible for following security policies and guidelines, and shall participate in developing those policies and guidelines when requested to do so.
- D. Passwords are an important element of computer security. A poorly chosen password may result in the compromise of the City's network. All City employees (including contractors and vendors with access to City systems) are responsible for taking appropriate steps to select and secure passwords. **Any activity performed under a user-id/password combination is presumed to have been performed by that user and is the responsibility of that user.**
- E. ITSD shall establish policies that address password use for Administrative User Accounts, Service Accounts and System-level Accounts.

**III. DEFINITIONS:**

- A. **Administrative User Account:** Any individually assigned user account that is used to perform technology related administrative functions or used in activities dealing with sensitive data (e.g. user management, network management, Oracle database administrator, SAP administrator).
- B. **Service Account:** Any account that is used for the operation or delivery of a technology service through an automated system.

- C. System-level Account: Any account that is necessary for the operation of a technology system (e.g., root, database administration accounts, NT admin, application administration accounts, etc.).
- D. User-level Account: Any assigned non-administrative user account (e.g., email, web, desktop computer, etc.)

**IV. POLICY GUIDELINES:**

This directive applies to all Technology Users who access the City's networks and any data and applications that reside on those networks.

**V. RESPONSIBILITIES:****Information Technology Services Department**

- A. Organizational responsibility for the development, implementation, maintenance, and compliance monitoring of this directive is placed with ITSD.
- B. ITSD will provide City departments with initial communication and training regarding this Directive. However, City Department Directors are ultimately responsible for communicating the policies and standards established in this directive to all personnel in their respective departments and for ensuring compliance within their respective departments with those policies and standards.
- C. ITSD is responsible for communicating the policies and standards established in this directive to all third-party users and for ensuring their compliance. Those City departments who work with the third-party users are responsible for identifying the third-party users to ITSD.
- D. ITSD reserves the right to terminate services to any user found in breach of this directive and if continued connectivity provides a threat to the City or City-administered technology or equipment. ITSD will attempt to contact the user's DSS prior to disconnecting the service as long as such notification does not allow further degradation of the City-administered technology or equipment. Such notification will be made after the disconnection if prior coordination was not possible.

**Department Directors and their designees**

- A. Supervisors shall ensure that employees and any affected third-party users (contractors, consultants, agencies having a contractual relationship with the City, part-time and temporary employees) have received a copy of this directive.
- B. Department Directors should ensure that no departmental personnel, including administrative staff, request access to or maintain lists or databases of other user's passwords.
- C. Department Directors are responsible for any disciplinary action taken against employees who violate this directive in accordance with paragraph VII. The Human

Resources Department will provide guidance as required to City departments regarding appropriate disciplinary action to be taken against employees who violate this policy.

**Employees**

- A. Employees are accountable for the proper use of City-owned technology, and should be aware that they are responsible for any information that they generate or distribute through the City's technology systems. Any activity performed on a workstation under an employee's login ID is presumed to be performed by that employee.
- B. Employees are responsible for complying with this directive, and with security policies and processes that may be developed by ITSD.
- C. Employees shall take reasonable and necessary care to prevent unauthorized access to workstations, laptops and other portable devices.
- D. Employees shall report any suspected security violation or threat to the ITSD Help Desk immediately.

**Human Resources Department**

- A. Human Resources will provide guidance to departments for disciplinary actions associated with violations of this directive.

**VI. PROCEDURES:**

- A. ITSD recommends the use of "strong" passwords. Strong passwords:
  - 1. Contain characters from three of the following four categories:
    - a) English uppercase characters (A through Z)
    - b) English lowercase characters (a through z)
    - c) Base 10 digits (0 through 9)
    - d) Non-alphanumeric characters (e.g., !, \$, #, %)
  - 2. Are at least 8 alphanumeric characters long.
  - 3. Are not words in any language, slang, dialect, or jargon.
  - 4. Are not based on personal information, such as the names of family.
  - 5. Are not common usage word such as:
    - a) Names of family, pets, friends, co-workers, fantasy characters, etc.
    - b) Computer terms and names, commands, sites, companies, hardware, software.
    - c) The words "COSA", "sananton" or any derivation.
    - d) Birthdays and other personal information such as addresses and phone numbers.
    - e) Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - f) Any of the above spelled backwards.

- g) Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- B. All user passwords will expire at intervals of ninety (90) days. Users will be prompted to change passwords beginning 10 days before the next expiration date.
- C. Passwords may not be re-used.
- D. Accounts will be "locked" after three (3) unsuccessful attempts to logon using a password. Users whose accounts have been locked must call the ITSD Help Desk to reset the user's password.
- E. Password Protection Guidelines for Users:
  - 1. Do not write passwords down, store them on-line, or reveal them in electronic communication.
  - 2. Do not use the same password for COSA accounts as for other accounts.
  - 3. Do not share COSA passwords with anyone. Passwords should be treated as sensitive, confidential COSA information.
  - 4. ITSD support personnel may require a user's password to resolve a problem. ITSD prefers that the user be present to enter a required password. If a password must be revealed to the technician, ITSD suggests that the password be changed as soon as is practicable.
  - 5. Do not talk about a password in the presence of others.
  - 6. Do not hint at the format of a password (e.g., "my family name").
  - 7. Do not reveal a password on questionnaires or security forms.
  - 8. Do not use the "Remember Password" feature of applications (e.g., websites, Outlook, and Netscape Messenger).
  - 9. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.
- F. If anyone other than ITSD support personnel requests a password from an employee, refer that person to the Information Technology Services Department to establish access to COSA systems and files as needed.
- G. ITSD is the only authorized password reset agent. ITSD support personnel may request information required to verify a user's identity.
- H. If an account or password is suspected to have been compromised, report the incident to ITSD and change all passwords.
- I. System, service, and other non-changeable passwords will be assigned and cataloged by ITSD. ITSD will take reasonable and necessary precautions to protect these passwords from compromise.

## **ADMINISTRATIVE DIRECTIVE 7.6**

## **Security and Passwords**

Effective Date: November 30, 2005

Revision Date(s):

### **VII. DISCIPLINE**

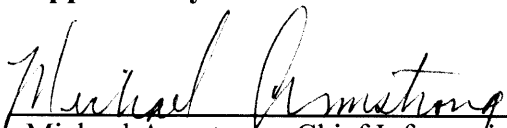
- A. Failure to comply with this directive will result in disciplinary action in accordance with the Municipal Civil Service Rules of the City of San Antonio, Rule XVII, Section 2. Discipline will be evaluated and based upon the number of violations and severity of the incident. The Human Resources Department must be consulted by a department when assessing the appropriate level of disciplinary action.
- B. Employees who fail to follow and administer this directive will be disciplined under the authority of the Department Director.
- C. This Administrative directive does not supersede the Department Director's authority over the determination of final disciplinary actions taken, particularly in cases where the safety of the general public or City employees are significantly compromised by an infraction of this administrative Directive. A Department Director may choose to assess more severe disciplinary action against an employee depending on the severity of the infraction.

**This directive supersedes all previous correspondence on this subject. Information and/or clarification may be obtained by contacting the ITSD Department at 207-8301.**

  
\_\_\_\_\_  
Hugh Millet, Jr., Interim Director ITSD

11/29/05  
\_\_\_\_\_  
Date

**Approved by:**

  
\_\_\_\_\_  
Michael Armstrong, Chief Information Officer

11/29/05  
\_\_\_\_\_  
Date

**Approved by:**

  
\_\_\_\_\_  
Sheryl Sculley, City Manager

11-29-05  
\_\_\_\_\_  
Date